UNIVERSIDAD POLITÉCNICA SALESIANA
SEDE QUITO

CARRERA:
INGENIERÍA DE SISTEMAS

Trabajo de titulación previo a la obtención del título de:
Ingenieros de Sistemas

TEMA:
"EVALUACIÓN DEL RENDIMIENTO DE HERRAMIENTAS ANTI-FORENSES EN CASOS EXPERIMENTALES MEDIANTE LA UTILIZACIÓN DE ESCENARIOS SIMULADOS"

AUTORES:
JULIO DAVID CÓNDOR CAIZA
EDISON ANDRES VILEMA CANGAHUAMIN

TUTOR:
JOSÉ LUIS AGUAYO MORALES

Quito, marzo 2019

CESIÓN DE DERECHOS DE AUTOR

Nosotros, JULIO DAVID CÓNDOR CAIZA, con documento de identificación N° 1712780632, y EDISON ANDRES VILEMA CANGAHUAMIN con documento de identificación N° 1723091516, manifestamos nuestra voluntad y cedemos a la Universidad Politécnica Salesiana la titularidad sobre los derechos patrimoniales en virtud de que somos autores del trabajo de titulación con el tema: "EVALUACIÓN DEL RENDIMIENTO DE HERRAMIENTAS ANTI-FORENSES EN CASOS EXPERIMENTALES MEDIANTE LA UTILIZACIÓN DE ESCENARIOS SIMULADOS", mismo que ha sido desarrollado para optar por el título de INGENIEROS DE SISTEMAS en la Universidad Politécnica Salesiana quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

En aplicación a lo determinado en la Ley de Propiedad Intelectual, en nuestra condición de autores reservamos los derechos morales de la obra antes citada.

En concordancia, suscribimos este documento en el momento que hacemos la entrega del trabajo final en formato impreso y digital a la Biblioteca de la Universidad Politécnica Salesiana.

JULIO DAVID
CÓNDOR CAIZA
CI: 1712780632

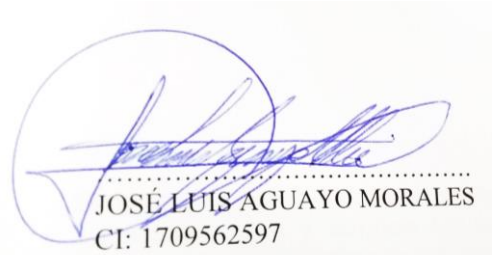
EDISON ANDRES
VILEMA CANGAHUAMIN
CI: 1723091516

Quito, marzo 2019

DECLARATORIA DE COAUTORÍA DEL TUTOR

Yo declaro que bajo mi dirección y asesoría fue desarrollado el Artículo Académico, con el tema: "EVALUACIÓN DEL RENDIMIENTO DE HERRAMIENTAS ANTI-FORENSES EN CASOS EXPERIMENTALES MEDIANTE LA UTILIZACIÓN DE ESCENARIOS SIMULADOS", realizado por Julio David Cóndor Caiza y Edison Andres Vilema Cangahuamin, obteniendo un producto que cumple con todos los requisitos estipulados por la Universidad Politécnica Salesiana, para ser considerado como trabajo final de titulación.

Quito, marzo 2019



JOSÉ LUIS AGUAYO MORALES
CI: 1709562597

Dedicatoria

Este artículo académico está dedicado a:
Mis padres Gonzalo y Mariana quienes con su amor, paciencia y esfuerzo me han permitido llegar a cumplir hoy un sueño más, gracias por inculcar en mí el ejemplo de esfuerzo y valentía, de no temer las adversidades porque Dios está conmigo siempre.
A mis hermanos por su cariño y apoyo incondicional, durante todo este proceso, por estar conmigo en todo momento gracias. A toda mi familia porque con sus oraciones, consejos y palabras de aliento hicieron de mí una mejor persona y de una u otra forma me acompañan en todos mis sueños y metas.

Julio David Cóndor Caiza

Dedico este trabajo a mis amados padres Clarita y Cesar, quienes con todo su esfuerzo, compresión, amor y sacrificio han sabido apoyarme incondicionalmente en cada momento de mi vida. Gracias a su ejemplo de trabajo duro, respeto y humildad han sembrado en mí todos los valores para ser una persona de bien y por ayudarme con todos los recursos para poder estudiar.

A mi hermano Gustavo Vilema, quien con su apoyo económico y sus consejos, me ayudó a cumplir el anhelo de estudiar en mi querida Universidad.

A todos mis hermanos, sobrinos y un ángel que tengo en el cielo J.F., por su ayuda y compañía ya que son una fuente de motivación, inspiración y felicidad.

A Karina la madre de mi hermosa hija, quien en este tiempo ha sabido amar, cuidar y velar por el bienestar de ella.

A mi pequeñita y amada hija Emilia Juliette, quien es mi tesoro y motor de superación profesional y personal.

Edison Andrés Vilema Cangahuamin

Agradecimiento

Quiero expresar mi gratitud a Dios, quien con su bendición llena siempre mi vida y a toda mi familia por estar siempre presentes.
Mi profundo agradecimiento a todas las autoridades y personal que hacen la Universidad Politécnica Salesiana, por confiar en mí, abrirme las puertas y permitirme realizar todo el proceso investigativo dentro de su establecimiento educativo.
Finalmente quiero expresar mi más grande y sincero agradecimiento al Ing. José Luis Aguayo, principal colaborador durante todo este proceso, quien con su dirección, conocimiento, enseñanza permitió el desarrollo de este trabajo.

Julio David Cóndor Caiza

Agradezco en primer lugar a Dios por haberme permitido llegar hasta este punto y haberme dado las fuerzas durante esta etapa de vida y además por regalarme una familia que siempre ha velado por mi superación profesional y personal. A toda mi familia quienes estuvieron siempre presentes con su apoyo incondicional durante toda mi vida.

Agradezco a la Universidad Politécnica Salesiana que ha contribuido en mi formación profesional y personal, a nuestro tutor de proyecto de titulación el Ing. José Luis Aguayo, quien con sus enseñanzas y tutorías contribuyó para desarrollar este trabajo.

Edison Andrés Vilema Cangahuamin

Evaluación del rendimiento de herramientas anti-forenses en casos experimentales mediante la utilización de escenarios simulados

Julio David Cóndor Caiza [#1]***, Edison Andrés Vilema Cangahuamin*** [#2]***, José Luis Aguayo Morales*** [*3]

Ingeniería de Sistemas, Universidad Politécnica Salesiana
Quito, Ecuador

[1]dcondorc@est.ups.edu.ec
[2]evilema@est.ups.edu.ec
[3]jaguayo@ups.edu.ec

Resumen- **El presente artículo se enfoca en la evaluación de las herramientas anti-forenses a través de la simulación de escenarios controlados que permiten conocer el rendimiento cuando se compromete la información a través del borrado seguro de archivos, que comúnmente puede ocurrir en un entorno real. Para ello se eligieron cuatro herramientas anti-forenses de borrado seguro bajo el criterio de compatibilidad con la plataforma Windows 10, que sean de distribución gratuita, que tengan interfaz gráfica y además que posean licencia pública. Las cuatro herramientas elegidas fueron: Hardwipe, Eraser, Secure Eraser, BitKiller. Estas herramientas de borrado seguro se ejecutaron en el sistema operativo Windows 10 y se realizaron las pruebas de rendimiento al borrar archivos almacenados en una unidad extraíble tipo flash. Para comprobar el borrado seguro de los archivos se realizaron los pasos dados por la informática forense con el fin de evidencias dejadas por cada herramienta. Para realizar la evaluación de las herramientas anti-forenses se utilizó el método comparativo y experimental y para evaluar el rendimiento se midió las métricas de tiempo de respuesta, el consumo de CPU y memoria durante el ataque con relación al tamaño total de archivos en MB (rendimiento=segundos/MB). Finalmente se compararon los resultados de cada evaluación dando como resultado a Hardwipe como la mejor herramienta de borrado seguro.**

Palabras Clave- **anti-forense, amenaza, sanitización, información, evidencia, atacante, incidente, hash, informática forense, borrado seguro, rendimiento.**

Abstract- T**his article focuses on the evaluation of anti-forensic tools through the simulation of controlled scenarios that allow to know the performance when the information is compromised through the secure deletion of files, which can commonly occur in a real environment. For this purpose, four anti-forensic erasure tools were chosen under the criterion of compatibility with the Windows 10 platform, which are free distribution, have a graphic interface and also have a public license. The four tools chosen were: Hardwipe, Eraser, Secure Eraser, BitKiller. These secure erase tools were run on the Windows 10 operating system and performance tests were performed when erasing files stored on a flash-type removable drive. In order to verify the safe erasure of the files, the steps taken by the forensic computer were carried out with the purpose of evidence left by each tool. To perform the evaluation of the anti-forensic tools, the comparative and experimental method was used and to measure the performance, the metrics of response time, CPU consumption and memory during the attack were measured in relation to the total size of files in MB (performance = seconds / MB). Finally, the results of each evaluation were compared, resulting in Hardwipe as the best safe erase tool.**

Keywords- **anti-forensic, threat, sanitization, information, evidence, attacker, incident, hash, computer forensics, secure erasure, performance.**

I. INTRODUCCIÓN

Hoy en día la información es uno de los mayores activos en una organización, por ende es muy importante protegerla de amenazas informáticas existentes que buscan afectar la integridad, confidencialidad y disponibilidad de los datos [1]. Por tal motivo es necesario comprender algunos conceptos sobre las técnicas anti-forenses debido a que son la antítesis a lo forense. Existen los delitos de robo de información que sustraen datos personales o de otra índole, donde la mayor parte de los autores son agentes internos que tienen acceso a la misma [2]. Un ejemplo es el ransomware, software malicioso, que restringe el acceso a la información que contiene un dispositivo mediante el cifrado haciéndole inutilizable, para luego pedir un pago a cambio de su recuperación [3]. Otro tipo de ataque es la sanitización digital que se basa en la técnica del borrado seguro donde el atacante elimina parcial o totalmente la información, sobrescribiendo a los archivos del dispositivo de almacenamiento que contiene la información. Las amenazas antes mencionadas son algunos delitos que diariamente cobran víctimas, por lo tanto el análisis forense digital es una rama crucial en la lucha contra los ataques informáticos [4]. Para esta investigación se seleccionó la técnica anti-forense de sanitización, que realiza un borrado seguro de archivos, carpetas o incluso puede hacer un borrado completo de un dispositivo de almacenamiento. Esta técnica se basa en la acción de sobrescritura con ceros y unos sobre la información contenida en un medio de almacenamiento para hacerla irrecuperable [5].

El avance de la tecnología ha permitido automatizar las técnicas anti-forenses mediante aplicaciones accesibles para personas mal intencionadas. Estas herramientas informáticas emulan las técnicas anti-forenses como: criptografía, sanitización, esteganografía y alteración de metadatos [4].

El presente trabajo se realizó por el interés de conocer el rendimiento de las herramientas anti-forenses de borrado seguro y poseer una fuente de información para los investigadores forenses y las personas que se están iniciando en el mundo del análisis forense. Existen un sin número de herramientas anti-forenses de borrado seguro y la falta de un estudio de evaluación, hace que no se pueda elegir una herramienta adecuada con sus tiempos de respuesta en un proceso de borrado, y por esta razón se tuvo la necesidad de realizar una comparación entre algunas herramientas.

A continuación se describen las cuatro herramientas anti-forenses de borrado seguro que se eligieron en esta investigación:

A. Hardwipe

Es una herramienta de sanitización de datos gratis compatible con Windows, puede borrar archivos, contenidos en carpetas, discos duros, dispositivos USB, y sanitizar la bandeja de reciclaje. Tiene las siguientes características: soporta múltiples lenguajes, puede borrar volúmenes enteros o solo particiones, genera reportes de la tarea procesada, soporta múltiples algoritmos de borrado, ayuda a liberar espacio en disco y es fácil de usar [6].

B. Eraser

Herramienta para Windows que permite borrar archivos, carpetas y medios de almacenamientos. Tiene las siguientes características: la tarea de borrado puede ser programada, soporta múltiples algoritmos de borrado [7].

C. Secure Eraser

Herramienta que sobrescribe la información hasta 35 veces, independientemente si son archivos, carpetas, unidades, papelera de reciclaje o rastros de navegación, trabaja en Windows, permite el método de arrastrar y pegar, es liviano, soporta múltiples algoritmos de borrado [8].

D. BitKiller

Borra de manera segura los archivos y directorios, puede sobrescribir de manera rápida, es portable por lo que no requiere instalación, se ejecuta en Windows, soporta múltiples algoritmos de borrado [9].

Para la evaluación de las herramientas de borrado seguro, se usaron los métodos comparativo y experimental, basándose en las tareas de la informática forense propuestas para este artículo. Se evaluaron los resultados obtenidos con la intensión de extraer determinadas conclusiones y hallar la mejor herramienta anti-forense por su rendimiento.

II. FUNDAMENTO TEÓRICO

A. Marco de Referencia

La evaluación del rendimiento de las herramientas anti-forenses, que se presentan en este artículo académico, se basa en la técnica anti-forense mencionada en el informe de Cyber Secured by ElevenPaths, donde se indica la detección de incidentes relacionados con la técnica de sanitización [10], y con base en ésta información, la técnica de sanitización fue sujeta a estudio. Las herramientas de sanitización elegidas y que mejor se adaptaron al presente artículo, debieron cumplir con los siguientes criterios: borrado de archivos, interfaz gráfica de usuario, licencia pública y en especial que se pueda ejecutar en la plataforma Windows como propone el autor Francisco Díaz [11].

Para realizar el ataque de borrado, los archivos fueron clasificados en cinco grupos: imágenes,

videos, archivos de audio, office, PDF. A través de un usuario mal intencionado se ejecutan las herramientas de sanitización para cada grupo, con el sistema operativo Windows 10, donde se registra el rendimiento de las herramientas, que según el autor Roger S. Presman [12] se debe medir el tiempo de respuesta y el uso de los recursos del sistema operativo con relación al tamaño total de archivos en MB (rendimiento=segundos/MB).

A través de la informática forense se hace una verificación de los archivos que fueron borrados. Utilizando la herramienta Autopsy y para no comprometer la evidencia digital, como indica autora Di Iorio Ana [13] se deben seguir los pasos para obtener el valor hash, realizar la imagen digital y el hash de la imagen digital para verificar que son copias idénticas. Para este artículo, con la distribución Kali Linux se registraron los tiempos de cada tarea en relación al tamaño de la unidad de almacenamiento en s/MB.

El aporte de la presente investigación es la evaluación del consumo de memoria, CPU y tiempo de borrado durante el ataque y con los resultados obtenidos comparar las cuatro herramientas que determinará la herramienta con mejor rendimiento.

Es importante conocer algunos conceptos acerca de las técnicas anti-forenses más relevantes, ya que en la actualidad un atacante puede manipular la información digital, cuándo un sistema informático ha sido vulnerado, distorsionado, escondido, destruido y por consiguiente al conocer sobre las técnicas anti-forenses puede encaminar con mejor criterio y tomar una mejor decisión en la investigación en el caso que se haya producido algún incidente de seguridad informática.

B. Método comparativo

Según [14] el método comparativo o el análisis comparativo es un procedimiento que se ubica entre los métodos científicos más utilizados por los investigadores. Junto con el método experimental y el estadístico, el método comparativo es un recurso ampliamente utilizado en la investigación científica.

El método comparativo tiene un punto de partida y una secuencia lógica divida en tres etapas. La primera etapa consiste en la configuración de una estructura teórica que sirva de apoyo para la elaboración de la hipótesis, lo cual debe extraerse de estudios y trabajos previos. Este marco conceptual debe definir las propiedades y características de los casos a comparar y debe permitir una cierta clasificación que identifique las variaciones y semejanzas del objeto de estudio, según sea el caso. En una segunda etapa, deberán definirse los criterios asumidos para la selección de la muestra, es decir de los casos a elegir como objeto de estudio. En este sentido debe estar plenamente justificada la selección, cuidando que los casos sean efectivamente comparables y relevantes. En una tercera etapa debe procederse al análisis de los casos fundamentalmente a partir de la comparación de las variables para determinar, las diferencias o las semejanzas.

C. Técnicas anti-forenses

Se caracterizan cuando un individuo logra afectar la información, en su disponibilidad, integridad o confiabilidad, con la finalidad de confundir cuando se realiza un análisis forense de las evidencias digitales y para evitar ser detectado en una investigación [15]. Facilitan a los atacantes informáticos y comprometen la información, debido a que alteran la evidencia digital e impiden la investigación normal de un delito informático [16]. De acuerdo a su forma de operar se pueden clasificar en cuatro tipos [17]:

1) *Criptografía:* Es una técnica que se utiliza para proteger los datos del atacante, paradójicamente el adversario en este caso sería el investigador forense. Está basada en las matemáticas avanzadas, complejidad computacional, probabilidad y estadística, alterando los mensajes, mediante el cifrado.

2) *Esteganografía:* Esta técnica anti-forense realiza el ocultamiento de un mensaje dentro de un objeto, que generalmente es: una imagen, un video o un archivo de audio de esta forma dicho mensaje pasa inadvertido para terceras personas.

3) *Sobrescritura Metadatos:* Esta técnica anti-forense altera los metadatos de un archivo o directorio para confundir la investigación en un análisis forense. Es bastante utilizada por un atacante dado que oculta sus pistas al sobrescribir sus propios tiempos de acceso a la información, de manera que un investigador no pueda construir una línea de tiempo confiable.

4) *Sanitización:* Es el proceso del borrado total o parcialmente de la información que se encuentra almacenada en un dispositivo con el objetivo que no pueda ser recuperado.

D. Herramienta anti-forense

Es una aplicación informática que busca la evasión o encubrimiento de huellas dentro de un delito informático. Han sido creadas por atacantes con el fin de automatizar y emular las técnicas anti-forenses como: borrado seguro, criptografía, esteganografía o alteración de metadatos. Estas herramientas permiten borrar el rastro o por lo menos confundir un delito con el objetivo de evitar que un investigador forense pueda llevar a cabo sus labores con éxito [18].

E. Evidencia digital

Según [19] la evidencia digital es la que se encuentra almacenada ya sea por campos magnéticos o pulsos electrónicos en un dispositivo y que puede ser analizado en una investigación. Es un término utilizado de manera amplia para describir cualquier registro generado por un sistema computacional de almacenamiento, que puede ser utilizado como evidencia de un proceso.

F. Informática Forense

A través de herramientas y técnicas disponibles, la informática forense es la encargada de la adquisición, análisis, preservación y la presentación de informes, cuando los medios de almacenamiento han sido procesados electrónicamente. Un técnico informático con ayuda de las tecnologías de la información y tareas como la adquisición, análisis, cotejo y preservación puede recuperar correctamente la evidencia digital, que se encentra tanto visible como oculta y en muchos casos reproducir el incidente ocurrido en una organización, con el objetivo de presentar dichas evidencias digitales ante órganos judiciales fortaleciendo el valor probatorio [13].

G. Sanitización

La técnica anti-forense de sanitización realiza el borrado parcial o total de la información almacenada en una unidad de almacenamiento digital, con el objetivo de no permitir la recuperación de la misma. La razón para utilizar esta técnica generalmente es la privacidad o seguridad sin embargo en algunos casos se usa para eliminar evidencia [17]. La sanitización conocida también como borrado seguro comprende la sobrescritura con patrones de ceros o unos a nivel de bit sobre los archivos, carpetas o toda la unidad de almacenamiento, con el propósito de imposibilitar la recuperación de la información.

H. Unidad de almacenamiento flash

Memorias flash tipo NAND son elementos electrónicos que almacenan datos, que pueden ser borrados y reprogramados. Una operación de escritura en un dispositivo flash solo se puede realizar en un bloque vacío o borrado, por lo que la operación de borrado debe preceder a la operación de escritura [20].

I. Virtualización

Es la técnica que permite instalar y ejecutar varios sistemas operativos en un mismo equipo físico mediante un programa por ejemplo VMware. En términos generales se emula un hardware que funciona como un servicio, un servidor o una red. De esta forma se crea lo que se conoce como una máquina virtual [21].

J. Sistema operativo Windows

El sistema operativo que se utilizó para realizar las pruebas de las herramientas anti-forenses fue Windows 10, en vista que ostenta el liderazgo en el mercado de sistemas operativos para ordenadores de escritorio y portátiles [22] con una interfaz amigable para el usuario.

K. Autopsy

Es la interfaz gráfica de la herramienta The Sleuth Kit, basado en GUI y que posee módulos de análisis forense digital, ofreciendo funciones esenciales como análisis del sistema de archivos y análisis de artefactos web. Permite la creación de informes completamente detallados y compatibles con otros sistemas según las necesidades del usuario investigador [23].

L. The Sleuth Kit

Desarrollado por @stake y The Coroner's Toolkit (TCT) es una herramienta forense digital de código abierto que contiene una biblioteca en C y una colección de líneas de comandos que permiten realizar la investigación de un disco duro [23].

M. El valor hash forense

Generar un hash SHA-1 (Secure Hahs Algoritmo 1), es una función criptográfica diseñada para producir un valor hash, interpretado como un número hexadecimal. Es utilizado en un proceso forense para la identificación, verificación y autenticación de su contenido en un medio de almacenamiento. Básicamente es una forma de verificar a través de un cálculo matemático, el contenido y así poder preservar la evidencia digital. Un cambio que se realice en los datos hará que también cambie el valor hash [24].

N. Data Carving

Es una técnica que permite identificar los archivos borrados de un medio de almacenamiento, mediante el análisis de su contenido, buscando a nivel de bit el formato específico de los archivos borrados. Utiliza un algoritmo de Header/Footer Carving el cual realiza una búsqueda de un header que indica el comienzo de un archivo y luego se añaden en secuencia los bytes contiguos hasta encontrar el footer que corresponde a ese tipo de archivo [25].

III. DESARROLLO

A. Pasos a seguir para la evaluación

Para elegir la herramienta anti-forense de sanitización con mejor rendimiento, se usó el método comparativo, para lo cual se tomaron como referencia los pasos que se adapten al escenario presentado en este artículo, según el autor Roger Pressman [12], el rendimiento se basa en la toma del registro del tiempo durante

la ejecución de los archivos que fueron borrados en la unidad de almacenamiento, adicionalmente menciona el consumo de memoria RAM y el consumo de CPU, que fueron tomados del administrador de tareas del sistema operativo Windows 10 respecto al tamaño total de los archivos en MB.

Una vez borrados los archivos con las herramientas de sanitización, mediante la informática forense se verifica qué sucedió con los archivos borrados. Según la autora Di Iorio Ana [13] sugiere los siguientes pasos para no comprometer la evidencia digital y que mejore se ajustaron al presente estudio y son: obtener el valor hash de la unidad de almacenamiento, realizar la imagen digital de la unidad de almacenamiento y obtener el valor hash de la imagen digital. Utilizando la distribución Kali Linux se realizaron los pasos antes mencionados y además se registró el tiempo de demora de cada uno. Posteriormente con la herramienta forense Autopsy se observa el reporte de los archivos borrados.

En la Figura 1, se muestra el esquema de los pasos que se siguió en este estudio.

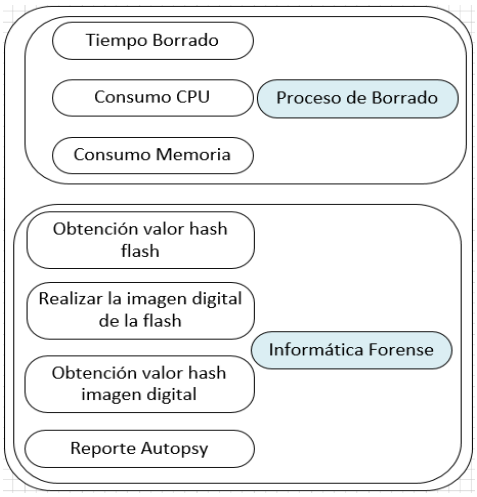


Figura 1. Pasos a seguir en este estudio.

B. Elegir la técnica anti-forense

Según el informe de Cyber Secured by ElevenPaths la técnica de sanitización fue descrita como una potente herramienta de borrado, debido a que fue capaz de borrar archivos importantes, sobre todo el master boot record de las unidades de almacenamiento.

En el 2015 se descubrieron ataques a sectores industriales en todo el mundo, que se han utiliza como una arma de extorsión digital. Desde enero 2018 se han descubierto incidentes graves relacionados con la sanitización frecuentemente en bancos de América Latina [10]. En base a esta información, la sanitización fue sujeta a estudio en este artículo.

C. Selección de herramientas anti-forenses

Haciendo una búsqueda en el internet de las herramientas de sanitización también conocidas como borrado seguro, se encontraron varias de éstas, las cuales se describen a continuación: DBan, Eraser, PC Disk Eraser, Hardwipe, Secure Eraser, KillDisk, HDSherdder, BitKiller [26].

Los criterios más relevantes fueron: la interfaz gráfica de usuario, que sean software libre, que permita borrar archivos, que se ejecute en plataforma Windows, y tenga licencia pública. Según [11] estos criterios se aplicaron al escenario propuesto en este artículo con las herramientas anti-forenses de sanitización que fueron seleccionadas.

En la tabla 1, se observan las herramientas que obtuvieron mejor puntuación: Eraser, Hardwipe, Secure Eraser y BitKiller, las mismas que fueron sujetas a la evaluación de su rendimiento.

Tabla 1. Criterios de selección para las herramientas Anti-forenses.

Factores	**Herramientas**							
Descripción	**DBan**	**Eraser**	**PC Disk Eraser**	**Hardwipe**	**Secure Eraser**	**KillDisk**	**Hd-sherdder**	**BitKiller**
Plataforma Windows	×	✓	×	✓	✓	×	×	✓
Interfaz GUI	×	✓	✓	✓	✓	×	×	✓
Licencia pública	✓	✓	✓	✓	✓	✓	✓	✓
Software libre	✓	✓	✓	✓	✓	✓	✓	✓
Borrado archivos	×	✓	×	✓	✓	×	×	✓
Deben cumplir todas	×	✓	×	✓	✓	×	×	✓

D. Escenario

Según el informe de Cyber Secured by ElevenPaths [10] los ataques de sanitización son direccionados a los archivos y según el informe de McAfee Lab [2] la mayor parte de los autores de los delitos informáticos son agentes internos. Por lo que se presentan los escenarios bajo los cuales se analizaron y compararon las cuatro herramientas anti-forenses utilizadas para este artículo en ambientes controlados sobre condiciones similares en un sistema real. Utilizando una máquina virtual con el programa VMware versión 12, con características de hardware de 4GB de memoria RAM, con 2 procesadores de 2.4 GHz, donde se instaló el sistema operativo Windows 10 Pro de 64 bit, el mismo que soporta otros programas y aplicaciones necesarias para su correcto funcionamiento, que se utiliza comúnmente en un ambiente de oficina. Desde el sistema operativo se ejecutaron las cuatro herramientas:

Hardwipe, Eraser, Secure Eraser, BitKiller para realizar el proceso de borrado seguro de los archivos almacenados en una unidad de almacenamiento tipo flash con capacidad de 4GB, conectada en el puerto USB de una portátil. Donde están almacenados 68 archivos con diferentes extensiones. Para la ejecución de las herramientas de sanitización se consideró un usuario mal intencionado, el cual realizó el borrado de los archivos en los siguientes casos.

1) Caso 1: Hardwipe.
2) Caso 2: Secure Eraser.
3) Caso 3: BitKiller.
4) Caso 4: Eraser.

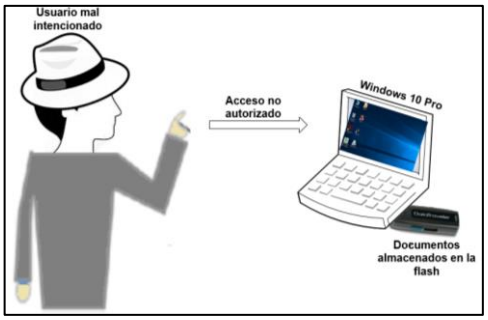


Figura 2. Escenario para la ejecución del borrado de archivos

E. Dispositivo atacado

En una unidad de almacenamiento tipo flash de marca Kingston Data Travel 2.0 USB Device, con capacidad de 4.096 MB y con un sistema de archivos FAT32, se almacenaron archivos como: procesador de texto, hojas de cálculo, presentación de diapositivas, archivos planos, pdf, imágenes, archivos de audio y videos que se muestran en la tabla 2.

Tabla 2. Archivos almacenados en la unidad Flash

Tipo de archivos	Tamaño total	Cantidad
Imágenes	447 KB	6
Videos	59,6 MB	2
Audio	39,9 MB	4
Office	24,4 MB	38
PDF	174 MB	18
Total archivos		68

F. Escenarios de ataques de borrado seguro

El ataque de borrado seguro se realizó individualmente, para los cuatro casos, donde se ejecutó desde la interfaz gráfica de usuario de cada herramienta de sanitización, borrando los archivos almacenados en la unidad tipo flash.

Las herramientas de borrado en su interfaz de usuario tienen la opción de elegir un algoritmo de sobrescritura y para los cuatro casos se utilizó el algoritmo llamado Random que sugiere el autor Aniello Castiglione en su trabajo [27] .

G. Ataque con Hardwipe

En la Figura 3, se observa la interfaz gráfica de usuario de la herramienta de borrado Hardwipe, la cual se ejecutó desde el sistema operativo Windows 10.

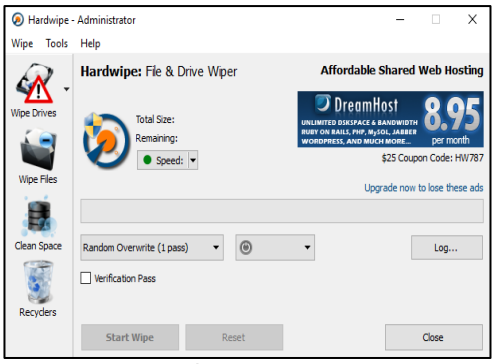


Figura 3. Ejecución de la herramienta Hardwipe.

H. Ataque con Secure Eraser

En la Figura 4, se observa la interfaz gráfica de usuario de la herramienta de borrado Secure Eraser, la cual se ejecutó desde el sistema operativo Windows 10.

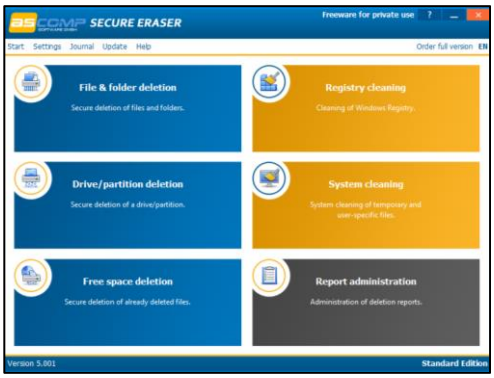


Figura 4. Ejecución de la herramienta Secure Eraser.

I. Ataque con BitKiller

En la Figura 5, se observa la interfaz gráfica de usuario de la herramienta de borrado BitKiller, la cual se ejecutó desde el sistema operativo Windows 10.

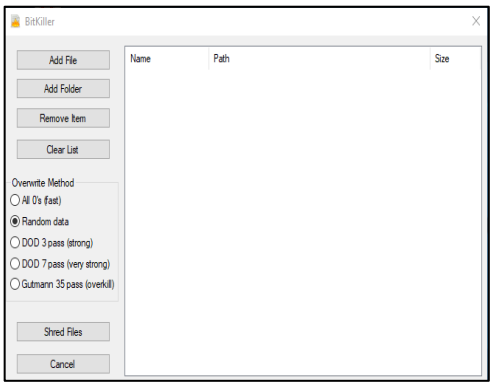


Figura 5. Ejecución de la herramienta BitKiller.

J. Ataque con Eraser

En la Figura 6, se observa la interfaz gráfica de usuario de la herramienta de borrado Eraser, la cual se ejecutó desde el sistema operativo Windows10.

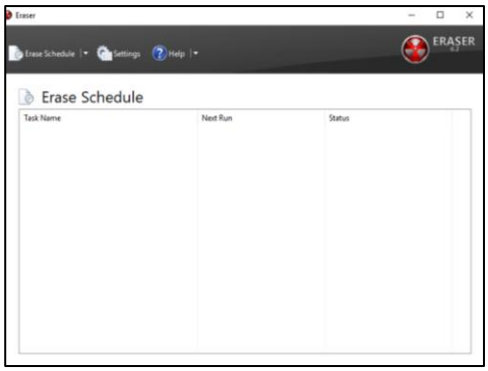


Figura 6. Ejecución de la herramienta Eraser.

IV. PRUEBAS Y RESULTADOS

La evaluación del rendimiento de las cuatro herramientas de borrado seguro, se realizó en base al tiempo del proceso de borrado, el uso de los recursos del sistema operativo Windows 10, registrando el consumo de memoria RAM, consumo de CPU, basado en el libro de Ingeniería de Software un Enfoque Práctico [12], que hace referencia al rendimiento.

Para comprobar el borrado seguro realizado por las cuatro herramientas se utilizó la informática forense [13].

A. Recursos del sistema operativo Windows 10

1) Tiempo del proceso de borrado

Se registró el tiempo que tardó la herramienta en el proceso de borrado de los archivos con las diferentes extensiones almacenadas en la unidad tipo flash. Dicho tiempo se tomó de las cuatro herramientas anti-forenses, como se describe en la tabla 3.

Tabla 3. Tiempo del proceso de borrado (Segundos)

Tipo de archivo	**Imagen**	**Office**	**Audio**	**Video**	**Pdf**	**Tiempo promedio**	**Tiempo total**	**Tiempo relativo al mínimo %**
Tamaño total	**0,44 MB**	**24,4 MB**	**39,9 MB**	**69,6 MB**	**174 MB**			
Hardwipe	5	23	9	12	36	26,49	85	100,00
Secure Eraser	10	60	93	129	398	275,20	690	811,70
BitKiller	6	38	12	16	56	40,58	128	150,50
Eraser	6	33	14	19	33	27,62	105	123,50

2) Consumo de memoria RAM

Una vez adicionados los diferentes archivos en cada herramienta para realizar el proceso de borrado, se observó en el administrador de tareas los recursos del sistema operativo demandados, como se describe en la tabla 4.

Tabla 4. Consumo de memoria RAM (MB)

Tipo de archivo	**(6) Imágenes**	**(38) Office**	**(4) Audio**	**(2) Videos**	**(18) PDF**	**TOTAL**
Tamaño total	**0,44 MB**	**24,4 MB**	**39,9 MB**	**59,6 MB**	**174 MB**	**298,34 MB**
Hardwipe	11,8	11,5	10,8	11,9	11,2	57,2
Secure Eraser	12,6	12,4	12,4	13,3	12,3	63,0
BitKiller	9,3	9,9	9,3	9,7	9,6	47,8
Eraser	26,8	28,2	24,9	24,1	24,9	128,9

3) Consumo de CPU

Luego de adicionar los archivos en las cuatro herramientas anti-forenses, se ejecuta el proceso de borrado, registrando el promedio de consumo del CPU, como se describen en la tabla 5.

Tabla 5. Consumo de CPU (%)

Tipo de archivo	**Imagen**	**Office**	**Audio**	**Video**	**Pdf**	**Total CPU (%)**	**Promedio aritmético**
Tamaño total	**0,44 MB**	**24,4 MB**	**39,9 MB**	**69,6 MB**	**174 MB**	**298,34 MB**	
Hardwipe	0.7	1.3	1.8	2.4	2.4	2.22	1.72
Secure Eraser	2.6	3.3	3.3	3.5	2.1	2.63	2.96
BitKiller	3.1	2.5	7.5	8.2	6.7	6.76	5.6
Eraser	3.3	2.3	2.9	4.8	4.2	3.98	3.5

B. Informática Forense

1) Obtención del valor hash de la unidad flash

Después del proceso de borrado de las cuatro herramientas anti-forenses, se utilizó la distribución Kali Linux y mediante la herramienta sha1sum se obtuvo el valor hash, consiguiendo como resultado un código único del contenido de la unidad de almacenamiento tipo flash, este código debe coincidir posteriormente con el valor hash de la imagen digital. La sintaxis que se utilizó es la que se muestra en la Figura 7.

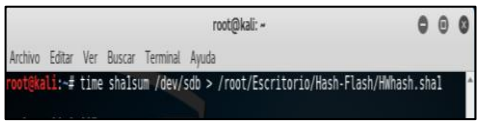


Figura 7. Sintaxis del valor hash del dispositivo.

2) Realizar la imagen digital de la unidad flash

Después de obtener el valor hash, nuevamente con la distribución Kali Linux, se utilizó la herramienta dd, que permite copiar desde el dispositivo de almacenamiento tipo flash de entrada hacia un archivo de salida. Este proceso permite realizar una réplica bit a bit, sector por sector dando como resultado la imagen digital la cual se va a manipular con la herramienta forense Autopsy. La sintaxis utilizada se muestra en la Figura 8.

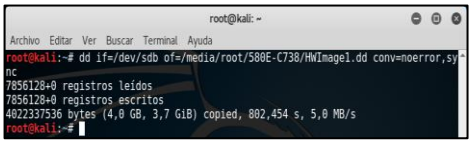


Figura 8. Sintaxis para obtenerla imagen del

3) Obtención del valor hash de la imagen digital

Después de sacar la imagen digital, con la distribución Kali Linux se utilizó nuevamente la herramienta sha1sum para obtener el valor hash, obteniendo un código único de la imagen digital el cual debe coincidir con el valor hash de la unidad de almacenamiento tipo flash. La sintaxis que se utilizó es la que se muestra en la Figura 9.

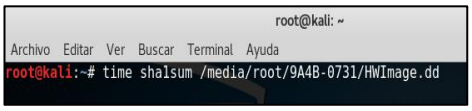


Figura 9. Sintaxis del valor hash de la imagen.

Una vez que se obtiene el valor hash de la unidad flash y el valor hash de la imagen digital, se compararon ambos valores los cuales deben coincidir, esto indica que el procedimiento se ha realizado correctamente y es factible analizar la imagen digital con la herramienta forense Autopsy. El resumen de la coincidencia de los valores hash, se describen en la tabla 6.

Tabla 6. Valor de la función hash de la unidad flash e imagen digital

Herramienta	Hash unidad flash	Hash imagen digital	Resultado
Hardwipe	331bb2114e 96fec4058b ca26092f10 697d9bb32b	331bb2114e 96fec4058b ca26092f10 697d9bb32b	Coincide
Secure Eraser	f14dc491ba 3d455dd420 2f80f1f73b 3a522255ba	f14dc491ba 3d455dd420 2f80f1f73b 3a522255ba	Coincide
BitKiller	52a111cbdf 8492fed76a 67fcbb9fd3 b116e22271	52a111cbdf 8492fed76a 67fcbb9fd3 b116e22271	Coincide
Eraser	3e121f1b48 74219ef9fd e09a30741e 88d3048e6b	3e121f1b48 74219ef9fd e09a30741e 88d3048e6b	Coincide

4) Reporte Autopsy

Con el software Autopsy versión 4.7.0 instalado en el sistema operativo Windows 10 y en una máquina física, se consiguió el reporte de los archivos que fueron identificados como borrado. Para lo cual se cargaron las imágenes digitales en Autopsy, seleccionando el módulo data carving se obtuvo el reporte de archivos clasificados en imágenes, videos, audio, office, PDF, como se describe en la tabla 7.

Tabla 7. Detalle del reporte de Autopsy de archivos borrados

Herramienta	(6) Imágenes Borrados	(38) Office Borrados	(4) Audio Borrados	(2) Videos Borrados	(18) PDF Borrados
Hardwipe	6	38	4	2	18
SecureEraser	6	38	4	2	18
BitKiller	12	74	8	4	36
Eraser	12	38	4	2	18

5) Comprobación del borrado seguro con la herramienta WinHex.

En la Figura 10, se observa la ejecución de la herramienta WinHex, y la apertura de un archivo almacenado en la unidad flash. Con el editor hexadecimal de WinHex se pudo observar el contenido del archivo antes del borrado seguro con Hardwipe

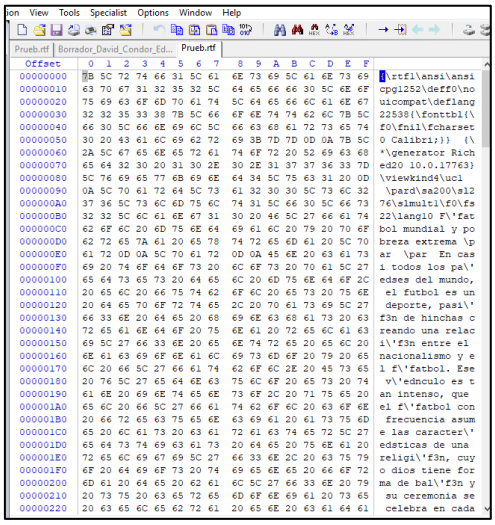


Figura 10. Visualización del contenido hexadecimal de un archivo antes del borrado seguro.

En la Figura 11, se observa el archivo resultante después del borrado seguro con Hardwipe, el contenido del archivo no fue posible recuperarlo.

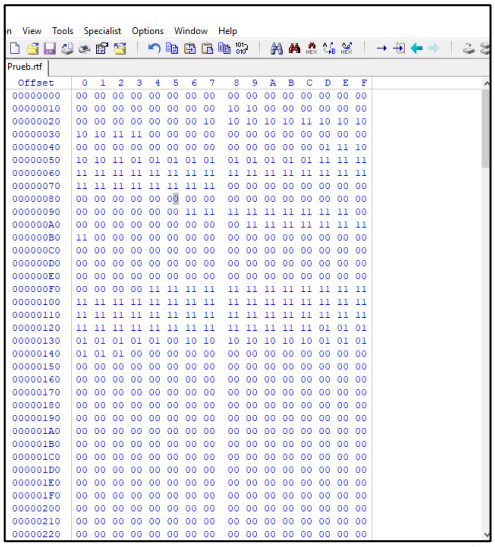


Figura 11. Contenido hexadecimal del archivo después del borrado seguro con Hardwipe.

V. Comparación de Resultados

Después de realizar las tareas propuestas en este artículo para la evaluación de las cuatro herramientas anti-forenses, se registraron los datos de las pruebas ejecutadas en base a los criterios de los recursos del sistema operativo Windows 10 y la informática forense obteniendo valores que se analizaron en las siguientes gráficas.

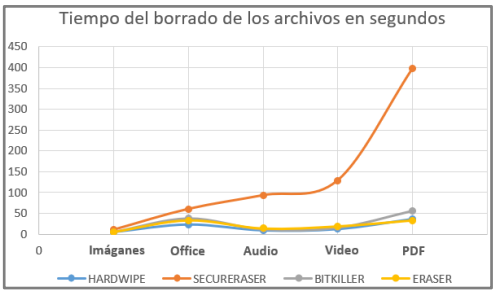


Figura 12. Tiempo del borrado de archivos.

En la Figura 12, se puede observar el tiempo que tardaron las cuatro herramientas anti-forenses para borrar los archivos de la unidad de almacenamiento tipo flash, donde Hardwipe fue la herramienta que menos tiempo tardó en realizar el proceso de borrado seguro de los archivos porque tuvo un tiempo de 5 segundos al borrar las imágenes que tenían un tamaño de 0,44MB, cuando realizó el borrado de los archivos de audio con un tamaño de 39,9 MB el tiempo que tardo fue de 9 segundos, cuando realizó el borrado de los archivos de video con un tamaño de 59,6 MB el tiempo que tardo fue de 12 segundos, cuando realizó el borrado de los archivos de office con un tamaño de 24,4 MB el tiempo que tardo fue de 23 segundos, estos datos que se registraron respecto al tiempo de borrado son los que menos tardaron con relación a las demás herramientas anti-forenses, cabe recalcar que Eraser tardó menos tiempo en el proceso de borrado seguro de los archivos PDF respecto a las demás herramientas.

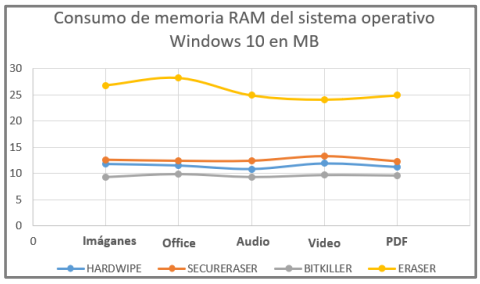


Figura 13. Consumo de memoria RAM.

En la Figura 13, se puede observar el consumo de memoria RAM del sistema operativo Windows 10 tomado del administrador de tareas, donde BitKiller es la herramienta anti-forense que consumió menos memoria al realizar el proceso de borrado seguro. Cuando se borraron los archivos de imágenes que tenían un tamaño de 0,44MB, el consumo de memoria fue de 9,3 MB, cuando se borraron los archivos de videos que tenían un tamaño de 59,6 MB el consumo de memoria fue de 9,7 MB, cuando se borraron los archivos de audio que tenían un tamaño 39,9 MB el consumo de memoria fue de 9,3 MB, cuando se borraron los archivos de office que tenían un tamaño de 24,4 MB el consumo de memoria fue de 9,9 MB, cuando se borraron los archivos de PDF que tenían un

tamaño de 174 MB el consumo de memoria fue de 9,6 MB.

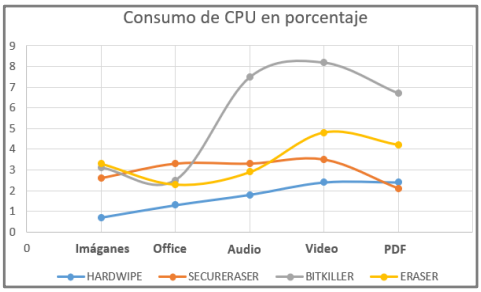


Figura 14. Consumo de CPU del sistema operativo Windows 10.

En la Figura 14, se puede observar el consumo promedio de CPU del sistema operativo Windows 10 tomado del administrador de tareas, donde Hardwipe fue la herramienta que menos consumo de CPU al realizar el proceso de borrado seguro respecto a las otras herramientas anti-forenses. Cuando se borraron los archivo de imágenes con un tamaño de 0,44 MB el consumo del promedio de CPU fue de 0,7%, cuando se borraron los archivos de videos con un tamaño de 59,6 MB el consumo del promedio de CPU fue de 2,4%, cuando se borraron los archivos de audio con un tamaño de 39.9 MB el consumo del promedio de CPU fue de 1,8%, cuando se borraron los archivos de office con un tamaño de 24,4 MB el consumo del promedio de CPU fue de 1,3%. Cabe destacar que Secure Eraser es la que menos consumió de CPU obtuvo respecto a las otras herramientas anti-forenses cunando se borraron los archivos de PDF que tenían un tamaño de 174 MB con un promedio de CPU de 2.1%.

Tabla 8. Rendimiento de las herramientas durante el proceso de borrado seguro

Tamaño Total / Herramienta	Imágenes 0,44 MB	Office 24,4 MB	Audio 39,9 MB	Video 59,6 MB	Pdf 174 MB
Hardwipe	11.36	0.94	0.23	0.20	0.21
SecureEraser	22.73	2.46	2.33	2.16	2.29
BitKiller	13.64	1.56	0.30	0.27	0.32
Eraser	13.64	1.35	0.35	0.32	0.19

En la tabla 8, se muestra la métrica del rendimiento en s/MB durante el proceso de borrado, donde Hardwipe es la herramienta que tuvo un mejor rendimiento con respecto a las otras herramientas al momento de realizar el proceso de borrado seguro. Cuando se borraron los archivos de tipo imágenes con un tamaño de 0,44 MB el rendimiento fue de 11,36 s/MB, cuando se borraron los archivos tipo office con un tamaño de 24,4 MB el rendimiento fue 0,94 s/MB, cuando se borraron los archivos de audio con un tamaño de 39.9 MB el rendimiento fue de 0,23 s/MB, cuando se borraron los archivos de tipo videos con un tamaño de 59,6 MB el rendimiento fue de 0,20 s/MB, cuando se borraron los archivos de tipo PDF con un tamaño de 174 MB el rendimiento fue de 0,21 s/MB.

VI. Discusión

Como se observa en los resultados obtenidos en el capítulo anterior, el ataque por borrado seguro con las cuatro herramientas genera alteraciones en los valores de los recursos del equipo en el que se ejecuten, estos valores pueden o no ser significativos ya que la manera de realizar el borrado de las cuatro herramientas es la misma. Por otro lado, el análisis forense de las imágenes digitales después del ataque puede servir de guía a los investigadores forenses en el caso que deban tomar acciones frente a un ataque de este tipo.

Es importante mencionar que el estudio fue posible gracias a varios recursos: primero a la liberación de las herramientas anti-forenses como open source presentados para efectos de estudio y análisis; segundo a las ventajas que ofrece la virtualización ya que permite evaluar diversos escenarios de experimentación sin la necesidad de emplear recursos físicos, reduciendo costos, tiempo y riesgos de pérdida de información; por último al libre acceso de la herramienta de simulación que permite analizar el comportamiento del virus dentro de una red real.

Tabla 9. Promedio total de las métricas durante el proceso de borrado

Herramienta	CPU	RAM	s/MB
Hardwipe	1.72	57.2	12.94
Secure Eraser	2.96	63	31.97
BitKiller	5.6	47.8	16.09
Eraser	3.5	128.9	15.85
Total	5.6	128.9	31.97

Finalmente, una vez realizadas las pruebas respectivas del ataque de borrado seguro con las cuatro herramientas, se realizó un promedio de las métricas y se trazó una línea de tendencia en donde se aprecia que Eraser genera un mayor impacto negativo en los recursos del equipo y además un mayor tiempo de demora en el proceso de borrado dando a notar mayor sospechas para un investigador forense, Hardwipe genera un impacto menor que las otras herramientas por tal motivo es la que tiene mejor rendimiento como se muestra en la Figura 15.

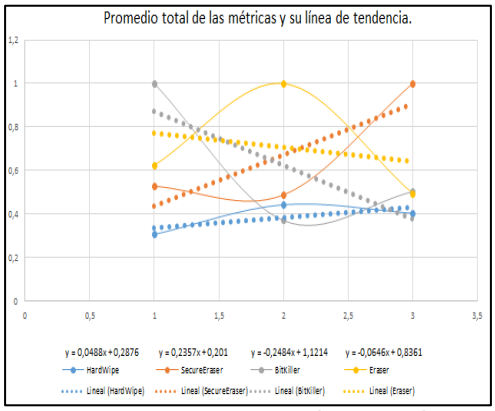


Figura 15. Promedio total de las métricas y su línea de tendencia.

VII. CONCLUSIONES

El borrado seguro es un ataque que busca eliminar archivos o información impidiendo a los usuarios el acceso y la recuperación de los mismos. Por lo tanto, el presente trabajo está orientado al análisis y evaluación del rendimiento de cuatro herramientas de borrado seguro en un escenario simulado con el fin de investigar medidas de seguridad para estos ataques.

Para la evaluación de las cuatro herramientas anti-forenses de borrado seguro de este artículo, fue necesario realizar los pasos de la informática forense, ya que así fue posible alcanzar mayores niveles de confiabilidad y relevancia al momento de deducir el comportamiento después del borrado seguro de los archivos de la unidad de almacenamiento.

Los archivos borrados con las herramientas anti-forenses de la unidad de almacenamiento fueron examinados a detalle con la herramienta forense Autopsy, con la cual se obtuvo como resultado que los archivos borrados sufrieron cambios en: sus metadatos, sus nombres y sus extensiones, con datos sin sentido haciéndoles ilegibles, irrecuperables y sobre todo confundiendo el análisis en la investigación.

La evaluación del rendimiento de las cuatro herramientas anti-forenses a través de los recursos del sistema operativo Windows 10, como el consumo de CPU y consumo de memoria, durante el proceso de borrado seguro determinó lo rápido que se realiza la tarea en condiciones particulares con respecto al tamaño total de los archivos borrados de la unidad de almacenamiento.

Después de conocer sobre las herramientas anti-forenses y ponerse en los zapatos de un atacante, este trabajo puede ayudar a construir una herramienta o mecanismos que sean menos propensos a estos ataques.

VIII. REFERENCIAS

[1] A. Carvajal, «Tecnologías globales para la segurdad de la información,» *GLOBALTEKSECURITY*, 2007.

[2] M. Labs, «Informe de McAfee Labs sobre amenazas,» 2016.

[3] U. d. Jaén, «Guías de seguridad UJA,» Jaén, 2018.

[4] N. Kumari, «Una visión de las ramas y herramientas forenses digitales.,» *IEEE Xplore Digital Library*, p. 8, 2016.

[5] R. Menjura Machado, «Informatica Forense,» 2012.

[6] Hardwipe, «Hardwipe Oficial,» Big Angry Dog, 2017. [En línea]. Available: https://www.hardwipe.com/.

[7] Eraser, «Eraser Oficial,» Eraser, Julio 2018. [En línea]. Available: https://eraser.heidi.ie/.

[8] SecureEraser, «Secure Eraser Oficial,» ASCOMP Software GmbH, 2017. [En línea]. Available: https://www.secure-eraser.com/.

[9] BitKiller, «sourceforge.net,» 2017. [En línea]. Available: https://sourceforge.net/projects/bitkiller/.

[10] Telefónica, «Impacto del malware de tipo wiper en Oriente Medio y América del Sur,» España, 2018.

[11] B. C. R. A. Díaz Francisco, «Evaluación de herramientas Free / Open Source para pruebas de software,» Buenos Aires, 2009.

[12] R. Pressman, Ingeniería de Software un enfoque práctico, Séptima ed., V. Pablo, Ed., México D.F.: Mc Graw Hill, 2010.

[13] A. Di Iorio , M. Castellote y B. Constanzo, El Rastro Digital del Delito aspectos técnicos, legales y estratégicos de la informática forense, J. M. Ravasi, Ed., Mar del Plata: Universidad Fasta, 2017.

[14] C. Gómez Díaz de León y E. A. León de la Garza, «Método Comparativo,» de *Métodos y técnicas cualitativas y cuantitativas aplicables a investigación en Ciencias Sociales*, T. Humanidades, Ed., México D.F., Tiran Humanidades, 2014, pp. 223-251.

[15] A. Botero , I. Camero y J. Cano , «Técnicas anti-forenses en Informática: Ingeniería reversa aplicada a TimeStomp,» *Criptored*, pp. 1-15, 2009.

[16] J. Anabalón y E. Donders, «Técnicas anti-forenses con VMware,» *Universidad Santiago de Chile*, pp. 1-8, 2012.

[17] M. Vasquez, «Técnicas anti-forenses Informáticas,» Marzo 2016. [En línea].

Available: https://rdu.unc.edu.ar/handle/11086/2849.

[18] D. Dittrich, «www.loquefaltaba.com,» 2017. [En línea]. Available: http://www.loquefaltaba.com/documentacion/forense/anti.html.

[19] J. Cano, «Introducción a la Informática Forense,» 2006. [En línea]. Available: http://52.0.140.184/typo43/fileadmin/Revista_96/dos.pdf.

[20] ITInsecurity, «insecurityit.blogspot.com,» 2013. [En línea]. Available: http://insecurityit.blogspot.com/2013/06/unidades-de-estado-solido-el-reto-de-la.html.

[21] A. Cursohacker, «cursohacker.es,» 2014. [En línea]. Available: http://cursohacker.es/que-es-la-virtualizacion-ventajas.

[22] U. Alicante, «Sistemas Operativos,» 2008. [En línea]. Available: https://rua.ua.es/dspace/bitstream/10045/54704/2/ci2_basico_2015-16_Sistemas_operativos.pdf.

[23] sleuthkit, «www.sleuthkit.org,» 2017. [En línea]. Available: http://www.sleuthkit.org/autopsy/.

[24] J. Hernández, «El dilema del algoritmo HASH,» *REVISTA DIGITAL SOBRE DIVULGACIÓN CRIMINALISTICA*, pp. 30-35, Enero 2016.

[25] B. Constanzo y J. Waimann, «El estado actual de las técnicas file carving y la necesidad de nuevas tecnologías que implementen carving inteligente,» *Universidad FASTA*, 2013.

[26] S. Sistemas, «Solvetic,» 3 Mayo 2017. [En línea]. Available: https://www.solvetic.com/page/recopilaciones/s/programas/programas-gratis-para-eliminar-borrar-disco-de-forma-segura. [Último acceso: 15 Julio 2017].

[27] A. Castiglione, G. Cattaneo y G. De Maio, «Eliminación automática, selectiva y segura de prubas digitales,» *IEEE Xplore Digital Library*, pp. 1-7, 2011.